Notice of Allowability	Application No.	Applicant(s)	
	10/763,673	PERRIOT, FREDERIC	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 7/23/2009*.

2. ☒ The allowed claim(s) is/are *3, 4, 6-19, 24-26, and 28-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20090804* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Randal D. Moran/
Examiner, Art Unit 2435

DETAILED ACTION

Claims 3, 4, 6-19, 24-26, and 28-30 are pending.

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Nikhil Iyengar on 7/15/2009.

The application has been amended as follows:

1-2. (Canceled)

3. (Previously Presented) The method of claim 6 wherein optimizing the decryption loop comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction.

4. (Original) The method of claim 3 wherein at least two of said techniques are combined synergistically.

5. (Canceled)

6. (Currently Amended) A computer-implemented method for determining whether computer code contains malicious code, said method comprising the steps of:

identifying computer code ~~suspected of currently containing malicious code, the computer code~~ having a decryption loop and a body;

performing a dead code elimination procedure on the computer code;

noting an amount of dead code eliminated during the dead code elimination procedure;

responsive to the amount of dead code eliminated during the dead code elimination procedure exceeding a preselected dead code threshold, declaring a suspicion of malicious code in the computer code;

optimizing the decryption loop to produce optimized loop code;

performing a malicious code detection procedure on the optimized loop code; and

~~optimizing the body to produce optimized body code;~~

~~subjecting the optimized body code to a malicious code detection protocol; and~~

responsive to the malicious code detection procedure detecting malicious code in the optimized loop code ~~or the malicious code detection protocol detecting malicious code in the optimized body code~~, declaring ~~a confirmation~~ that the computer code contains malicious code.

7. (Original) The method of claim 6 wherein the malicious code detection procedure is a procedure from the group of procedures consisting of pattern matching, emulation, checksumming, heuristics, tracing, and algorithmic scanning.

8. (Currently Amended) The method of claim [[6]] 29 wherein the malicious code detection protocol is a protocol from the group of protocols consisting of pattern matching, emulation, checksumming, heuristics, tracing, X-raying, and algorithmic scanning.

9. (Currently Amended) The method of claim [[6]] 29 wherein the step of optimizing the body comprises using at least one output from the group of steps consisting of optimizing the decryption loop and performing a malicious code detection procedure on the optimized loop code.

10. (Currently Amended) The method of claim [[6]] 29 wherein, when the step of performing a malicious code detection procedure on the optimized loop code indicates the presence of malicious code in the computer code, the steps of optimizing the body and subjecting the optimized body code to a malicious code detection protocol are aborted.

11. (Original) The method of claim 6 further comprising the additional step of, after the step of performing a malicious code detection procedure on the optimized loop code, revealing an encrypted body.

12. (Original) The method of claim 11 wherein the step of revealing an encrypted body comprises emulating the optimized loop code.

13. (Original) The method of claim 11 wherein the step of revealing an encrypted body comprises applying a key gleaned from the optimized loop code.

14. (Previously Presented) The method of claim 6, wherein optimizing the decryption loop to produce optimized loop code comprises:

performing a forward pass operation;

performing a backward pass operation;

performing a control flow graph reduction; and

iterating the above three steps a plurality of times.

15. (Original) The method of claim 14 wherein the iteration of the three steps stops after either:

a preselected number of iterations; or

observing that no optimizations of the computer code were performed in the most recent iteration.

16. (Original) The method of claim 14 further comprising the step of performing a code motion procedure, wherein the four steps are iterated a plurality of times.

17. (Previously Presented) The method of claim 14 wherein the forward pass operation comprises one or more steps from the set consisting of:

peephole optimization;

constant folding;

copy propagation;

forward computations related to abstract interpretation; and

instruction specialization.

18. (Previously Presented) The method of claim 14 wherein the backward pass operation comprises one or more steps from the set consisting of backward computations related to abstract interpretation and local dead code elimination.

19. (Original) The method of claim 18 wherein the backward pass operation comprises the additional step of global dead code elimination.

20-23. (Canceled)

24. (Currently Amended) A computer-readable storage medium containing executable computer program instructions for determining whether computer code contains malicious code, said computer program instructions performing the steps of:

identifying computer code ~~suspected of currently containing malicious code, the computer code~~ having a decryption loop and a body;

performing a dead code elimination procedure on the computer code;

noting an amount of dead code eliminated during the dead code elimination procedure;

responsive to the amount of dead code eliminated during the dead code elimination procedure exceeding a preselected dead code threshold, declaring a suspicion of malicious code in the computer code;

optimizing the decryption loop to produce optimized loop code;

performing a malicious code detection procedure on the optimized loop code; and

~~optimizing the body to produce optimized body code;~~

~~subjecting the optimized body code to a malicious code detection protocol; and~~

responsive to the malicious code detection procedure detecting malicious code in the optimized loop code ~~or the malicious code detection~~

~~protocol detecting malicious code in the optimized body code~~,

declaring ~~a confirmation~~ that the computer code contains malicious code.

25. (Currently Amended) The computer-readable medium of claim 24 wherein the malicious code detection ~~protocol~~ procedure is a ~~protocol~~ procedure from the group of ~~protocols~~ procedures consisting of pattern matching, emulation, checksumming, heuristics, tracing, X-raying, and algorithmic scanning.

26. (Previously Presented) The computer-readable medium of claim 24 wherein optimizing the decryption loop comprises performing at least one technique from the group of techniques consisting of constant folding, copy propagation, non-obvious dead code elimination, code motion, peephole optimization, abstract interpretation, instruction specialization, and control flow graph reduction.

27. (Canceled)

28. (Previously Presented) The method of claim 6 wherein the malicious code detection procedure comprises emulating the optimized loop code.

29. (New) The method of claim 6, further comprising:

optimizing a body of the computer code to produce optimized body code;

subjecting the optimized body code to a malicious code detection protocol; and

responsive to the malicious code detection protocol detecting malicious code in the optimized body code, declaring that the computer code contains malicious code.

30. (New) The computer-readable medium of claim 24, wherein the computer program instructions are for further performing the steps of:

optimizing a body of the computer code to produce optimized body code;

subjecting the optimized body code to a malicious code detection protocol; and

responsive to the malicious code detection protocol detecting malicious code in the optimized body code, declaring that the computer code contains malicious code.

Allowable Subject Matter

Claims 3, 4, 6-19, 24-26, and 28-30 are allowed.

The following is an examiner's statement of reasons for allowance: The prior art discloses converting a program to a "standardized version" that expresses the function of the program and using this standardized version for malware detection. Nachenberg describes a method for detecting a polymorphic virus using emulation. Nachenberg discloses emulating a decryption loop to decrypt a virus body so that the decrypted body can be compared to known viruses. Nachenberg discloses reducing the number of instructions to be emulated, but this reduction is not done through code optimization.

The prior art fails to teach "optimizing the decryption loop to produce optimized loop code," or "performing a malicious code detection procedure on the

optimized loop code." The prior art describes examining sequences of instructions during emulation to determine if those sequences are likely part of a decryption loop (e.g., the sequences contain "boosters"). If it is determined that the sequences are not likely part of a decryption loop, emulation can be stopped. Christodorescu discloses creating a standardized version of a program and comparing the standardized version to standardized malicious code portions. Neither portion discloses optimizing a decryption loop and performing a malicious code detection procedure on the optimized code in combination with performing a dead code elimination procedure on the computer code; noting an amount of dead code eliminated during the dead code elimination procedure; responsive to the amount of dead code eliminated during the dead code elimination procedure exceeding a preselected dead code threshold, declaring a suspicion of malicious code in the computer code.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435